PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00 — A1

(11) International Publication Number: **WO 00/07088**

(43) International Publication Date: 10 February 2000 (10.02.00)

(21) International Application Number: PCT/US99/17315

(22) International Filing Date: 29 July 1999 (29.07.99)

(30) Priority Data:
09/127,218 31 July 1998 (31.07.98) US

(71) Applicant: DURANGO CORPORATION [US/US]; 57 Gates Street, Framingham, MA 01702 (US).

(72) Inventors: RALLIS, William, N.; 57 Gates Street, Framingham, MA 01702 (US). BEHAR, Yaacov; 83 Church Street, Winchester, MA 01890 (US).

(74) Agents: BARBAS, Charles, J. et al.; Cesari and McKenna, LLP, 30 Rowes Wharf, Boston, MA 02110 (US).

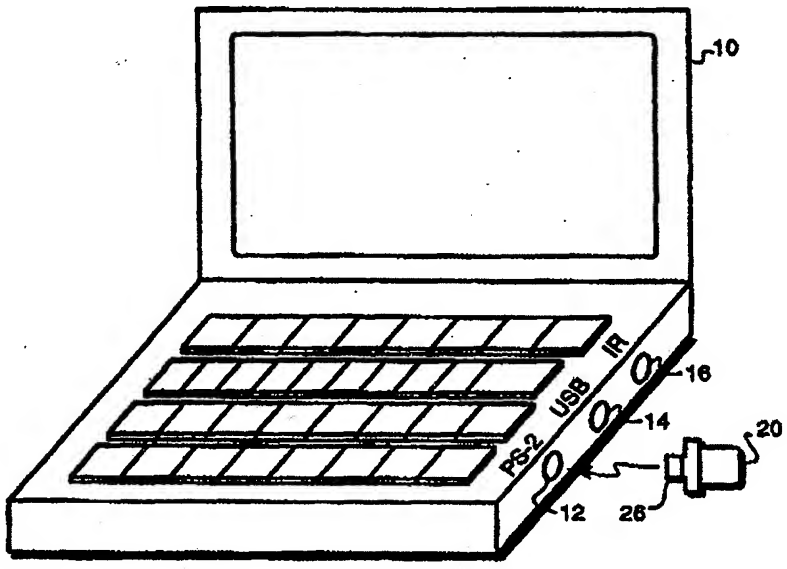
(81) Designated States: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA, UZ, VN, YU, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: NOTEBOOK SECURITY SYSTEM (NBS)

(57) Abstract

A multi–level security system prevents unauthorized use of a computer. The system has a key device carrying a first serial number, a mass storage device installed in the computer and storing a validation record, the validation record having a copy of the first serial number. The computer is automatically powered down if the first serial number and the copy of the first serial number do not match. Also the key device may carry an encryption key. The computer has a device to store a copy of a second serial number. The validation record has an encrypted portion, the encrypted portion carrying an encrypted copy of the second serial number. The computer is automatically powered down if the copy of the second serial number and a decrypted copy of the second serial number do not match. Also, the validation record may carry a personal identification number (validation record PIN). A user to enters an entered version of a PIN (entered PIN). The computer is automatically powered down if the validation PIN and the entered PIN do not match. The key device may carry an access code (key device access code). The validation record has a copy of the access code (validation access code). The validation access code is written to the key device, the key device having means for comparing the key device access code to the validation access code. The computer is powered down if the key device access code and the validation access code do not match. Any combination of a subset of these security measures may be used.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

3NSDOCID: <WO_____0007088A1_I_>

NOTEBOOK SECURITY SYSTEM (NBS)

BACKGROUND OF THE INVENTION

This is a continuation-in-part of U.S. Application Serial No. 09/022,088, filed February 11, 1998 and incorporated herein by reference.

Theft is a serious and expensive problem for the users of notebook, or laptop, computers. It has been estimated that over a quarter of a million notebook computers are stolen each year, and a majority of business firms report losses from notebook computer theft. In addition to the value of the hardware, users may also suffer the loss of data stored on the computers. Conventional methods for protecting computer hardware consist of either physically isolating the computer in a locked room or mechanically securing the computer to a fixed object. However, such devices are cumbersome to use and defeat the mobility of the notebook computer.

There are notebook computer security systems that electronically track a computer and sound an alarm when it is moved a certain distance from the user. However, users will often disarm such security features because they restrict personal movement, and passersby will typically ignore audible alarms and similar warning devices. Another security system is a password program that directs the computer to secretly dial a security company when an improper password is entered. The security company uses the caller ID feature to locate the computer. This system may be defeated by intercepting the outgoing call. Other security devices, such as "smart cards" and dongles, are also available, but these devices are designed for the protection of data and not for the deterrence of theft of computers.

Therefore, what is needed is an easy-to-use and low cost security system to deter the theft of a notebook computer.

3NSDOCID: <WO_____0007088A1_I_>

SUMMARY OF THE INVENTION

Briefly, a security system constructed in accordance with the invention implements a user-validation procedure that requires the user to connect the proper hardware "key" device to a computer at power-up to enable operation. The system can support multiple users and a single supervisor. Each authorized user is provided with a unique key device which is carried and stored separately from the computer. The key device holds a unique serial number and an encryption key. A validation record stored on the computer's hard disk contains an unencrypted key device serial number, an encrypted hard disk serial number, and a Personal Identification Number (PIN) unique to the user.

A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device.

Because the key device is not required for normal computer operations, after the user-validation procedure has successfully terminated, the user can remove the key device and keep it separate from the computer. Moreover, the small size of the key device makes it easy to transport and keep safe.

3NSDOCID: <WO_____0007088A1_I_>

BRIEF DESCRIPTION OF THE DRAWINGS

The above and further advantages of the invention may be better understood by referring to the following description in conjunction with the accompanying drawing, in which:

Fig. 1A is an illustration of the Notebook Security System (NBS);

Fig. 1B is an illustration of a key device;

Fig. 2 is a block diagram of the major components within the CPU address space of an IBM-PC compatible computer;

Fig. 3 is a flow diagram of the boot and user-validation procedure;

Figs. 4A - 4C depict the PS2/USB interface protocol;

Figs. 5A - 5F illustrate various key device-to-computer interfaces;

Figs. 6A - 6B illustrate various IR key device configurations;

Fig. 7 depicts the IR interface message framing format;

Fig. 8 is a block diagram of the software partitioning of an IBM-PC compatible computer; and

Fig. 9 is a depiction of the user screen of the user-validation program application.

DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

Fig. 1A shows a key device 20 connected to a notebook computer 10. The key device 20, shown in Fig. 1B, has no external controls and is comprised of a microcomputer 22, a read-only-memory 24 and a connector 26. The connector 26 may attach to one of the I/O ports on the notebook computer 10. The preferred key device connection is via a PS-2 connector 12, although alternative connections, such as a Universal Serial Bus (USB) 14 and an Infra-Red (IR) port 16, can be used as described below. Although the security system has been designed for use with a notebook computer 10, it will be recognized that the system can be adapted for use with other computers, such as a desktops or Personal Digital Assistants (PDA).

Ideally, the key device 20 is of such shape and size as to be placed on the user's key chain. It receives power and command messages from the notebook computer 10

3NSDOCID: <WO_____0007088A1_|_>

and returns response messages, a serial number and an encryption key. A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user. For maximum security protection, the key device 20 is connected only during the user-validation procedure and is carried and stored separately from the notebook computer 10.

Fig. 2 is a block diagram of the major components within the Central Processing Unit (CPU) 50 address space for a conventional IBM PC-compatible computer. At power-up, the CPU 50 accesses the Basic Input/Output System (BIOS) Read-Only Memory (ROM) 30 and executes a "boot-up" procedure. Prior to the termination of the boot-up procedure, the CPU downloads the operating system (OS) program via a memory-mapped interface 40 from a mass storage device, such as a hard drive 42 or possibly a diskette 44, and reads it into main Random-Access Memory (RAM) memory 60. In the preferred embodiment of the invention, the boot-up user-validation program resides in a ROM adapter 34 of the BIOS 30 and is executed at boot-up and prior to the download of the operating system.

A flow diagram of the user-validation procedure is shown in Fig. 3. In Step 1, the user-validation program prompts the user to attach the key device 20 to the notebook computer 10. The program attempts to communicate with the key device 20 for a fixed delay period. If a key device 20 is not detected within this period, then the program proceeds to Step 11 where the computer is automatically powered down. In Step 2, the program reads the key device serial number and encryption key that are stored in the key device ROM 24. The key device serial number and encryption key, usually a large prime number, are loaded into the key device 20 by the manufacturer.

The protocol for interfacing the key device 20 to the computer 10 through a PS-2 port 12 or a USB port 14 is shown in Fig. 4. The first portion, shown in Fig. 4A, is the standard, or conventional, initialization protocol flow between the notebook computer 10 and either a keyboard 46 or a mouse 48. After power up or a *reset* (FF) command from the BIOS, the device will identify its type ("AA" = keyboard; "AA 00" =

3NSDOCID: <WO_____0007088A1_I_>

mouse). A *read identification* (F2) command is then issued and a keyboard 46, for example, will return an *acknowledgment* (FA) response and the "AB 41" identification number.

A novel protocol for reading the key device data through a PS-2 or USB port is shown in Figure 4B. After the initialization protocol is executed, the key device 20 waits for a unique two-command sequence that it will recognize as the cue for sending the key device serial number and encryption key. For illustrative purposes, the sequence is shown as an *echo* (EE) command followed by a *read identification* (F2) command. The program sends an *echo* (EE) command to the key device 20. The key device 20 returns an *echo* (EE) response. After the echo test bits have been verified, the program issues a *read identification* (F2) command to the key device 20. The key device 20 returns an *acknowledgment* (FA) response and the "AB 41" identification number and further appends the key device serial number and encryption key. In this example, the key device 20 appends the serial number and encryption key only when the *read identification* (F2) command is immediately preceded by the *echo* (EE) command.

In Step 3, the program compares the key device serial number to the corresponding number in a set of stored validation records, one of which is maintained for each user. The records are stored in a reserved sector of the hard disk 42, or other mass storage device, preferably when the security system software is installed on the computer. Each validation record is comprised of the following fields:

FIELD 1 -- key device serial number (standard ASCII characters)
FIELD 2 -- personal identification number (PIN) (encrypted)
FIELD 3 -- internal device serial number (encrypted)
FIELD 4 -- level: user or supervisor (encrypted)
FIELD 5 -- user encryption keys (encrypted)
FIELD 6 -- user information (encrypted)

If the key device serial number received from the key device 20 does not match field 1 of any of the validation records, then the program proceeds to Step 11.

In Step 4, the program uses the encryption key to decrypt the encrypted portions of the validation record. If the decrypted record reads as plain ASCII text, the program

3NSDOCID: <WO_____0007088A1_I_>

moves to Step 5, otherwise, it proceeds to Step 9. In Step 5, the user-validation program prompts the user to enter a PIN. The PIN consists of a string of six to eight characters. In Step 6, the program compares the PIN to the corresponding number stored in field 2 of the decrypted validation record. If the numbers do not match, the program moves to Step 11. If the system is configured to operate without the manual entry of a password or PIN, Steps 5 and 6 are bypassed.

At Step 7, the program reads the serial number of an internal device, preferably the hard disk 42. The retrieved serial number is compared to the plain text serial number of field 3 of the validation record. If the serial numbers match, the user has been validated. If the numbers do not match, the program moves to Step 11.

In Step 10, the program waits for the key device 20 to be disconnected from the notebook computer 10. It periodically executes the read protocol of Fig. 4B to determines whether the key device serial number and encryption key data are appended to the *acknowledgment* (FA) response. When the key device data is not appended to the *acknowledgment* (FA) response, the program terminates and normal computer operations can commence.

In a multiple user situation, a supervisor is designated by setting the single bit of field 4 of the validation record. If the bit is set, the supervisor can gain access to the users' encryption keys which are stored in field 5. The user information in field 6 holds user-specific data stored for informational purposes.

To provide protection against the copying of the serial number and encryption key data from the key device 20, a "super key" access code procedure may be programmed by the manufacturer into the key device 20, and a "super key" verification step may be inserted at the start of the user validation procedure. The access code procedure requires the key device 20 to verify receipt of a matching code number before it will output the serial number and encryption key data. Preferably, the access code "hops", or changes, each time the key device 20 is accessed.

A novel protocol for writing data to the key device 20 through a PS-2 port 12 or a USB port 14 is shown in Figure 4C. The write protocol is executed after the initiali-

3NSDOCID: <WO_____0007088A1_I_>

zation protocol of Fig. 4A and prior to the read protocol of Fig. 4B. The key device 20 waits for a unique two-command sequence that it will recognize as the signal that the program is sending one byte of data. For illustrative purposes, the sequence is shown as two consecutive *echo* (EE) commands. After the echo test bits are verified, the program issues a *low nibble* (0X0; X = low nibble data) data message to the key device 20. The key device 20 returns an *acknowledgment* (FA) response. The program next issues a *high nibble* (0Y0; Y = high nibble data) data message to the key device 20 and the key device 20 again returns an *acknowledgment* (FA) response.

The "super key" access code number that is sent by the program to the key device 20 may be longer than one byte. The write protocol of Fig. 4C is repeated as necessary for each additional byte of data. The key device 20 microprocessor 22 concatenates the low and high nibbles and compares the resulting number to the access code number stored in its memory 24. If the numbers do not match, the key device 20 will not append the serial number and encryption key data to the *acknowledgment* (FA) response as shown in Fig. 4B.

Alternative physical connections can be employed to connect the key device 20 to a notebook computer 10 as shown in Fig. 5. Any serial or parallel port may be used, although the PS-2 and USB port connections, shown respectively in Fig. 5A and 5B, are preferred because of their small size. As an alternative to serial number and encryption key data, the key device 20 can include special security features, such as a finger print reader 28 (Fig. 5C), or a "smartcard" reader that senses data on a "smartcard" 29 (Fig. 5D), to generate key data. This data is forwarded by the key device 20 to the user-validation program in a manner identical to the transmission of serial number and encryption key data.

In another alternative a PS-2 "Y" connector 13, equipped with an internal automatic switch (not shown), is employed to permit the simultaneous PS-2 connection of a key device 20 and a keyboard 46 (or mouse 48) to a notebook computer 10 as shown in Fig. 5E. In a similar alternative, the key device 20 is connected to the keyboard port 18 of a desktop computer 11 via a AT "Y" connector 19, equipped with an internal auto-

BNSDOCID: <WO_____0007088A1_I_>

matic switch (not shown), that also permits the simultaneous connection of an AT keyboard 47 as shown in Fig. 5F.

The internal automatic switch (not shown) in each "Y" connector is controlled by an internal microprocessor (not shown). The switch is configured to be normally open at the key device port and normally closed at the "pass-through" port of each "Y" connector. The microprocessor monitors the transmissions across the switch. When it detects the protocol command sequences described above, it temporarily switches the connection to the key device port and relays the command and response messages between the computer 10 and the key device 20. The switch automatically reverts back to pass-through mode when the computer 10/key device 20 communications are completed.

In an alternative interface, the IR key device 21 is equipped for Infrared (IR) communications with a notebook computer 10 via the IR port 16 as shown in Fig. 6A. Ideally, the IR key device 21 is of such shape and size as to be placed on the user's key chain. It is self-powered and in its basic configuration, as shown in Figure 6B, includes an IR transmitter 27 and a momentary transmit switch 25, in addition to a microprocessor and ROM (not shown). When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the *Ultra* Protocol as established by the Infrared Data Association (IrDA).

The *Ultra* Protocol for exchanging messages between the IR key device 21 and the computer 10 through the IR port 16 is documented in "Infrared Data Association Guidelines for *Ultra* Protocols" which is incorporated by reference. The message framing and layer specific headers are shown in Figure 7. The IR key device 21 utilizes a frame 70 identified by a unique Protocol Identification (PID) field 71 value, e.g. 02h, assigned and reserved by IrDA. The key data resides in the variable length protocol data field 72. The frame size is specified in the Frame Check Sequence (FCS) field 73 which is CRC-CCITT (Cyclic Redundancy Check - International Telegraph and Telephone Consultative Committee; CRC with polynomial equal to $X^{16} + X^{12} + X^5 + 1$) er-

INSDOCID: <WO_____0007088A1_I_>

ror correction encoded. Note that all occurrences of the end-of-file (EOF) value (e.g. C1h) in the FCS field 73 are changed to prevent a premature EOF detection.

In the "super key" configuration, the IR key device 21 includes both an IR transmitter and IR receiver, but does not include a transmit switch. The IR key device 21 remains the powered-down state until it receives an IR pulse. After the user-validation program prompts the user to align the IR key device 21 with the IR port 16, it transmits a command message containing a "super key" access code number. The access code procedure requires the IR key device 21 to verify receipt of a matching code number before it will output the serial number and encryption key data. Preferably, the access code "hops", or changes, each time the IR key device 21 is accessed. If the IR key device 21 verifies a match between the received access code and a number stored within the device, it transmits a response message containing the key device serial number and the encryption key.

As an alternative to serial number and encryption key data, the IR key device 21 can include special security features, such as a finger print reader 28 (Fig. 6C), or a "smartcard" reader that senses data on a "smartcard" 29 (Fig. 6D), to generate the key data. This data is forwarded to the user-validation program in a manner identical to the IR transmission of the serial number and encryption key data, although a new PID is assigned to each new configuration.

In another alternative, a PS-2/IR "Y" connector 17, equipped with an internal automatic switch (not shown), is employed to permit the simultaneous IR connection of an IR key device 21 and a keyboard 46 (or mouse 48) to a notebook computer 10 as shown in Fig. 6E.

Alternate physical configurations of the key device 20 are also possible. The key device 20 may be implemented as a Personal Computer Memory Card Industry Association (PCMCIA) card , a floppy diskette, or by any other detachable means for providing a key device serial number and an encryption key to the notebook computer 10.

As an added feature of the invention, an application program that implements the user-validation procedure may be installed with the security system and, preferably,

3NSDOCID: <WO_____0007088A1_I_>

on a Microsoft Windows 95/98/NT/CE platform. The application will provide either (user selected) automatic hard disk lock-up or computer power-down that triggers during normal operation after expiration of a user-defined inactivity period. The application also supports manual initiation of lock-up or power-down. In cases where the ROM BIOS program is not installed, the application can be used to prevent unauthorized user access to the hard disk contents.

To support the application on the Windows 95/98/NT/CE platform, an Operating System Interface (OSI) is provided. The application 92 is interfaced to the operating system 100 via an Application Program Interface (API) layer 90 as shown in Fig. 8. The OSI is comprised of two parts: the key device driver 112 and the OS visual interface. Within the I/O subsystem 104 an interface layer 110 supports various drivers, such as a disk driver 114, a key device driver 112, and a network driver 116. The key device driver 112 provides the application interface to the key device 20. It reads the key device serial number and the encryption key, matches the key device serial number to that of the validation record stored on the hard disk, and uses the encryption key to decrypt the encrypted portion of the validation record.

An OS visual interface is illustrated in Fig. 9-. The interface is comprised of a display window 82 for displaying messages to the user during the user-validation procedure or setting program parameters, a task bar "key" object 84 to either lock/unlock the hard disk or power-down the computer, a "key" icon 86 in the control panel for adjusting program parameters, and a "vault" object 88 to indicate whether the hard disk is locked or not (e.g. the vault door is either closed or open).

It is desirable that some form of warning label be applied to the exterior of the notebook computer 10 to deter a would-be thief. Such a practice is common with home burglary systems. The label should state that the computer is protected by a security system that will not permit operation without a special key device.

The utility of the invention is not limited to deterrence of computer hardware theft. For example, the key device 20 may also be used as a new and improved "dongle" for software copy protection. A dongle is a hardware security device that at-

3NSDOCID: <WO_____0007088A1_I_>

taches to an I/O port, typically the parallel port, of a computer and contains a unique key number. To protect against software theft, third party applications 91 may require retrieval of a key, such as that stored in a dongle, to permit execution. With little or no modification, the key device 20 may be used as a dongle. In addition, software developers may incorporate into their applications the user validation procedure and PS-2/USB/IR communications protocols described above.

The foregoing has been limited to specific embodiments of this invention. It will be apparent, however, that variations and modifications may be made to the embodiments, with the attainment of some or all of their advantages. Therefore, it is the object of the appended claims to cover all such variations and modifications as come within the true spirit and scope of the invention.

What is claimed is:

CLAIMS

1. A multi-level security system to prevent unauthorized use of a computer, said system comprising:

a key device carrying a first serial number;

a device installed in said computer and storing a validation record, said validation record having a copy of said first serial number;

an interface to connect said key device to said computer and to provide a pathway to read said first serial number;

a computer program to compare said first serial number from said key device to said copy of said first serial number; and,

means for automatically powering down said computer if said first serial number and said copy of said first serial number do not match.

2. The security system of claim 1 further comprising:

said key device carrying an encryption key;

said computer having a device to store a copy of a second serial number;

said validation record having an encrypted portion, said encrypted portion carrying an encrypted copy of said second serial number;

said computer program to decrypt said second serial number from said validation record using said encryption key, to produce a decrypted version of said second serial number, and to compare said decrypted version of said second serial number with said copy of said second serial number; and,

means for automatically powering down said computer if said copy of said second serial number and said decrypted copy of said second serial number do not match.

3. A multi-level security system to prevent unauthorized use of a computer, said system comprising:

a key device carrying a first serial number and an encryption key;

at least one device installed in said computer and storing a validation record, said validation record having a copy of said first serial number and said validation rec-

3NSDOCID: <WO_____0007088A1_I_>

ord having an encrypted portion, said encrypted portion carrying an encrypted copy of a second serial number;

an interface to connect said key device to said computer and to provide a pathway to read said first serial number and said encryption key;

a computer program to compare said first serial number from said key device to said copy of said first serial number;

said computer having a device to store a copy of a second serial number;

said computer program to decrypt said second serial number from said validation record using said encryption key, to produce a decrypted version of said second serial number, and to compare said decrypted version of said second serial number with said copy of said second serial number;

means for automatically powering down said computer if said first serial number and said copy of said first serial number do not match; and,

means for automatically powering down said computer if said copy of said second serial number and said decrypted copy of said second serial number do not match.

4. The security system of claim 1 further comprising:

said validation record carrying a personal identification number (validation record PIN);

a keyboard for a user to enter an entered version of a PIN (entered PIN);

a computer program to compare said validation PIN with said entered PIN;

means for automatically powering down said computer if said validation PIN and said entered PIN do not match.

5. A security system as in claim 1 further comprising:

said key device carrying an encryption key;

said computer having a device to store a copy of a second serial number;

said validation record having an encrypted portion, said encrypted portion carrying an encrypted copy of said second serial number and an encrypted version of a user personal identification number (encrypted PIN);

said computer program to decrypt said second serial number from said validation record using said encryption key, to produce a decrypted version of said second serial number, and to compare said decrypted version of said second serial number with said copy of said second serial number,

said computer program to decrypt said encrypted PIN to produce a decrypted PIN;

a keyboard for a user to enter an entered version of a PIN (entered PIN); and,

means for automatically powering down said computer if said copy of said second serial number and said decrypted copy of said second serial number do not match OR said decrypted PIN and said entered PIN do not match.

6. The security system of claim 1 further comprising:

said key device carrying an access code (key device access code);

said validation record having a copy of said access code (validation access code);

means for writing said validation access code to said key device, said key device having means for comparing said key device access code to said validation access code; and,

means for automatically powering down said computer if said key device access code and said validation access code do not match.

7. The security system of claim 1 wherein said computer program resides in a BIOS ROM adapter of said computer.

8. The system of claim 1 wherein said interface is a PS-2 port.

9. The system of claim 1 wherein said interface is a USB port.

10. The system of claim 1 wherein said interface is an Infrared port.

3NSDOCID: <WO_____0007088A1_I_>

11. A multi-level security system to prevent unauthorized use of a computer, said system comprising:

a key device carrying a first serial number;

a mass storage device installed in said computer and storing a validation record, said validation record having a copy of said first serial number;

an interface to connect said key device to said computer and to provide a pathway to read said first serial number;

a computer program to compare said first serial number from said key device to said copy of said first serial number;

means for automatically powering down said computer if said first serial number and said copy of said first serial number do not match.

said key device carrying an encryption key;

said computer having a device to store a copy of a second serial number;

said validation record having an encrypted portion, said encrypted portion carrying an encrypted copy of said second serial number;

said computer program to decrypt said second serial number from said validation record using said encryption key, to produce a decrypted version of said second serial number, and to compare said decrypted version of said second serial number with said copy of said second serial number;

means for automatically powering down said computer if said copy of said second serial number and said decrypted copy of said second serial number do not match;

said validation record carrying a personal identification number (validation record PIN);

a keyboard for a user to enter an entered version of a PIN (entered PIN);

a computer program to compare said validation PIN with said entered PIN;

means for automatically powering down said computer if said validation PIN and said entered PIN do not match;

said key device carrying an access code (key device access code);

said validation record having a copy of said access code (validation access code);

means for writing said validation access code to said key device, said key device having means for comparing said key device access code to said validation access code; and,

means for automatically powering down said computer if said key device access code and said validation access code do not match.

12. A method for securing a computer comprising the steps of:

carrying a first serial number in a key device;

storing a validation record in a mass storage device installed in said computer, said validation record having a copy of said first serial number;

providing a pathway to read said first serial number through an interface to connect said key device to said computer;

comparing said first serial number from said key device to said copy of said first serial number by a computer program; and,

powering down said computer if said first serial number and said copy of said first serial number do not match.

13. The method of claim 12 further comprising:

carrying an encryption key in said key device;

storing a copy of a second serial number in a device in said computer;

carrying an encrypted copy of said second serial number in said validation record;

decrypting said second serial number from said validation record using said encryption key, to produce a decrypted version of said second serial number;

comparing said decrypted version of said second serial number with said copy of said second serial number; and,

powering down said computer if said copy of said second serial number and said decrypted copy of said second serial number do not match.

14. A method for securing a computer comprising the steps of:

carrying a first serial number and an encryption key in a key device;

3NSDOCID: <WO_____0007088A1_I_>

storing a copy of a second serial number in a device in said computer;

storing a validation record in at least one storage device installed in said computer, said validation record having a copy of said first serial number, and having an encrypted version of said second serial number;

providing a pathway to read said first serial number and said encryption key through an interface connecting said key device to said computer;

comparing said first serial number from said key device to said copy of said first serial number;

decrypting said second serial number from said validation record using said encryption key, to produce a decrypted version of said second serial number;

comparing said decrypted version of said second serial number with said copy of said second serial number;

powering down said computer if said first serial number and said copy of said first serial number do not match; and,

powering down said computer if said copy of said second serial number and said decrypted copy of said second serial number do not match.

15. The security method of claim 12 further comprising:

carrying a personal identification number (validation record PIN) in said validation record;

entering an entered version of a PIN (entered PIN) into said computer by a user;

comparing said validation PIN with said entered PIN;

powering down said computer if said validation PIN and said entered PIN do not match.

16. A method as in claim 12 further comprising:

carrying an encryption key in said key device;

storing a copy of a second serial number in said computer;

carrying an encrypted copy of said second serial number and an encrypted version of a user personal identification number (encrypted PIN) in said validation record;

3NSDOCID: <WO_____0007088A1_I_>

decrypting said second serial number from said validation record using said encryption key, to produce a decrypted version of said second serial number;

comparing said decrypted version of said second serial number with said copy of said second serial number,

decrypting said encrypted PIN to produce a decrypted PIN;

entering an entered version of a PIN (entered PIN) by a user; and,

powering down said computer if said copy of said second serial number and said decrypted copy of said second serial number do not match OR said decrypted PIN and said entered PIN do not match.

17. The method of claim 12 further comprising:

carrying an access code in said key device (key device access code);

carrying a copy of said access code in said validation record (validation access code);

writing said validation access code to said key device, said key device comparing said key device access code to said validation access code; and,

powering down said computer if said key device access code and said validation access code do not match.

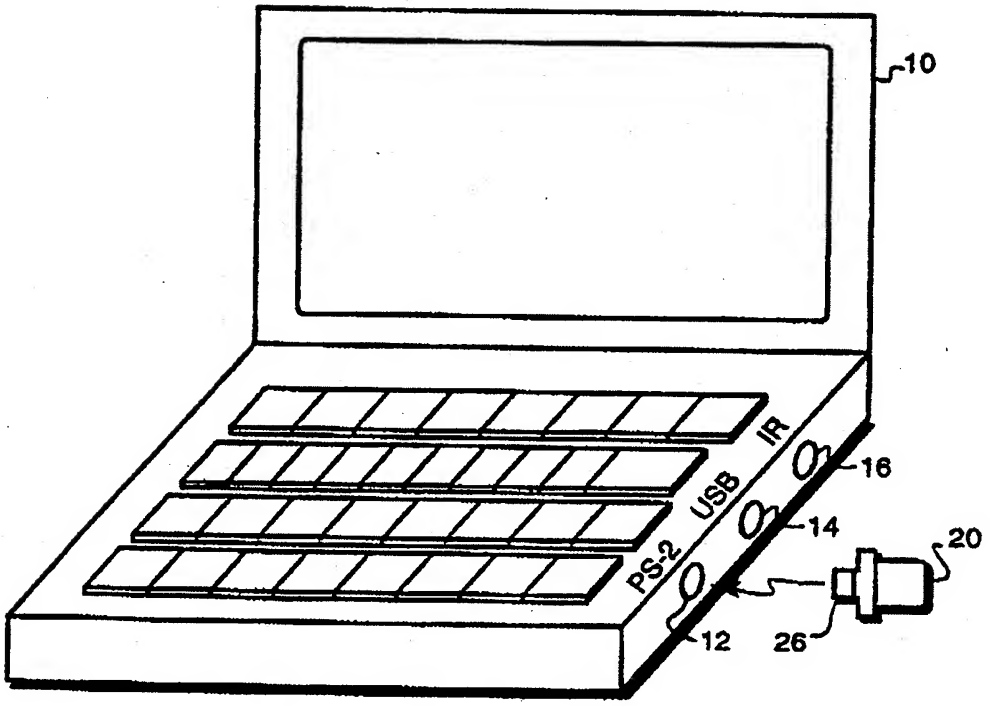


FIG. 1A

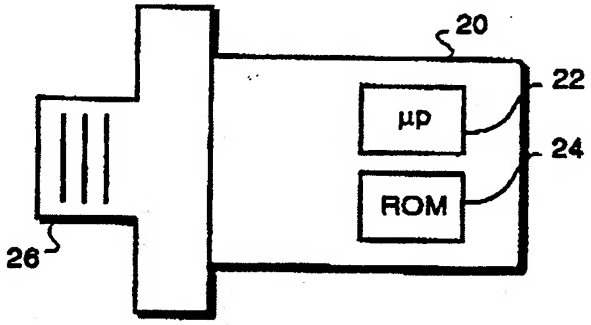


FIG. 1B

3NSDOCID: <WO_____0007088A1_I_>

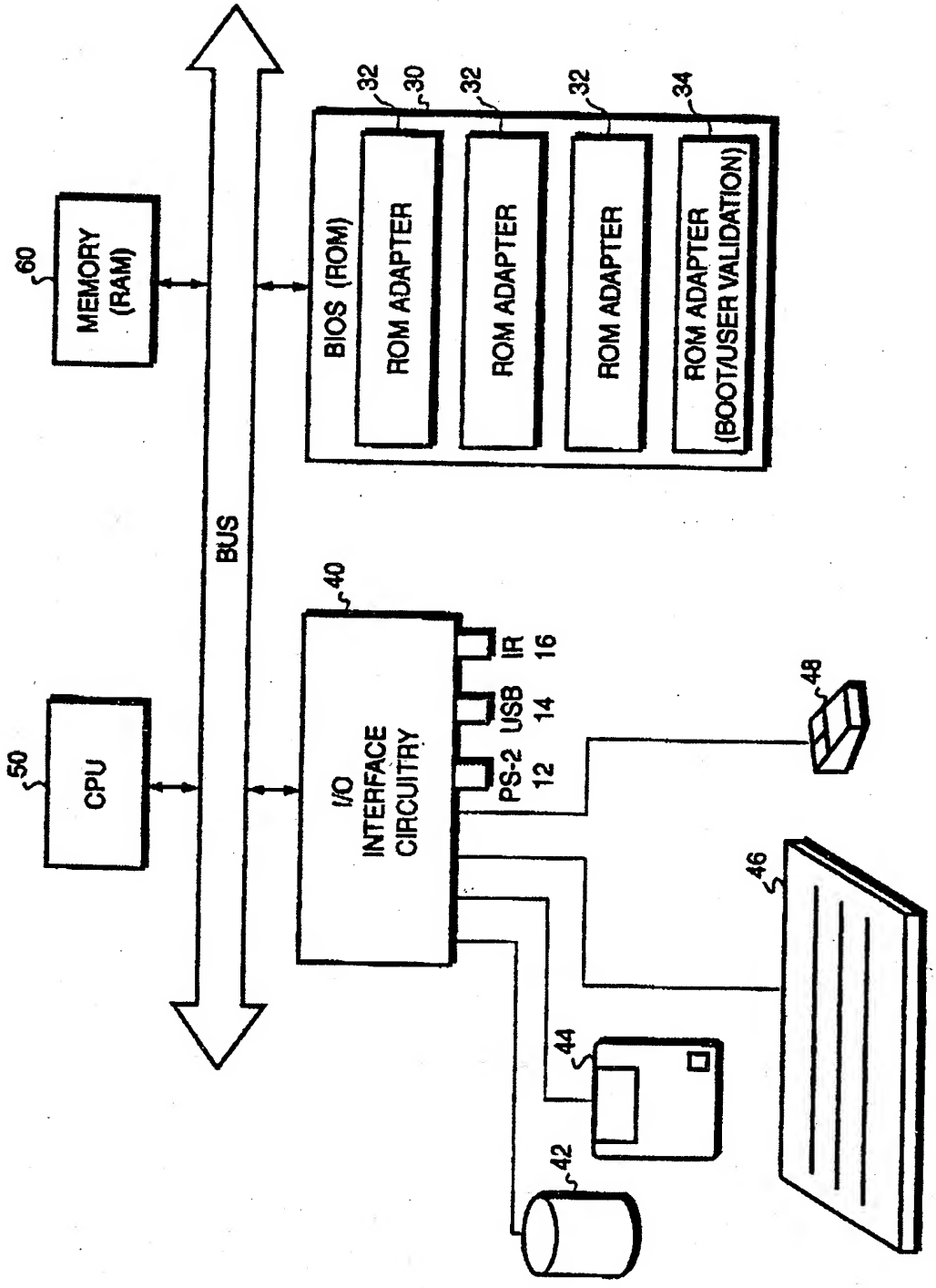


FIG. 2

3NSDOCID: <WO_____0007088A1_I_>

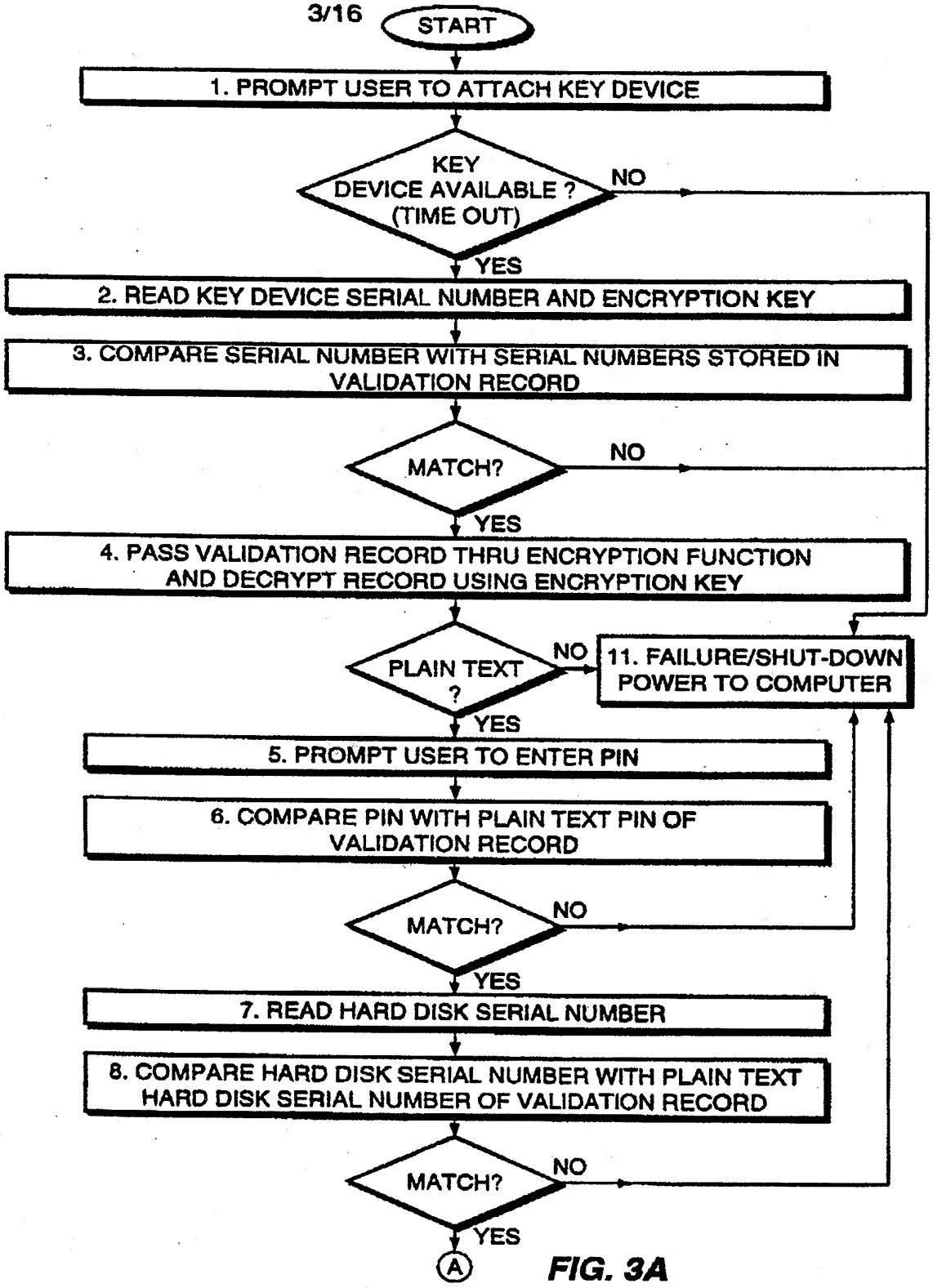


FIG. 3A

BNSDOCID: <WO_____0007088A1_I_>

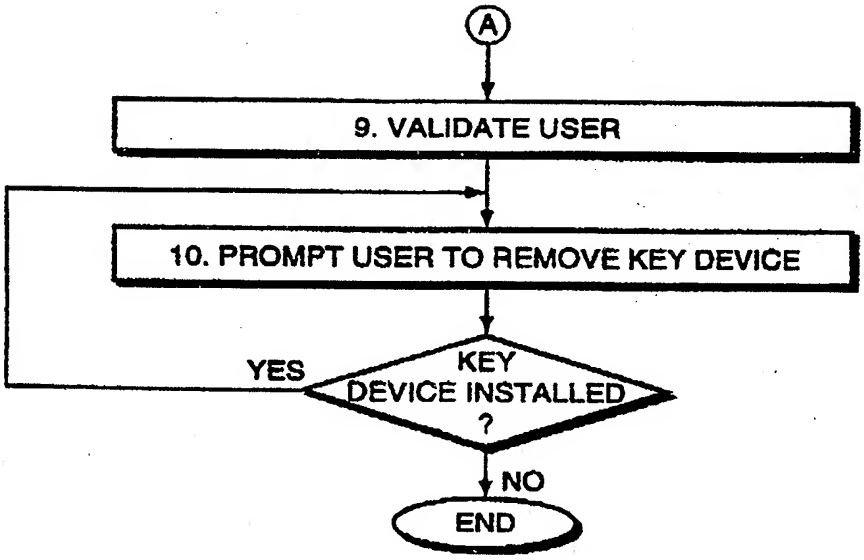


FIG. 3B

3NSDOCID: <WO_____0007088A1_I_>

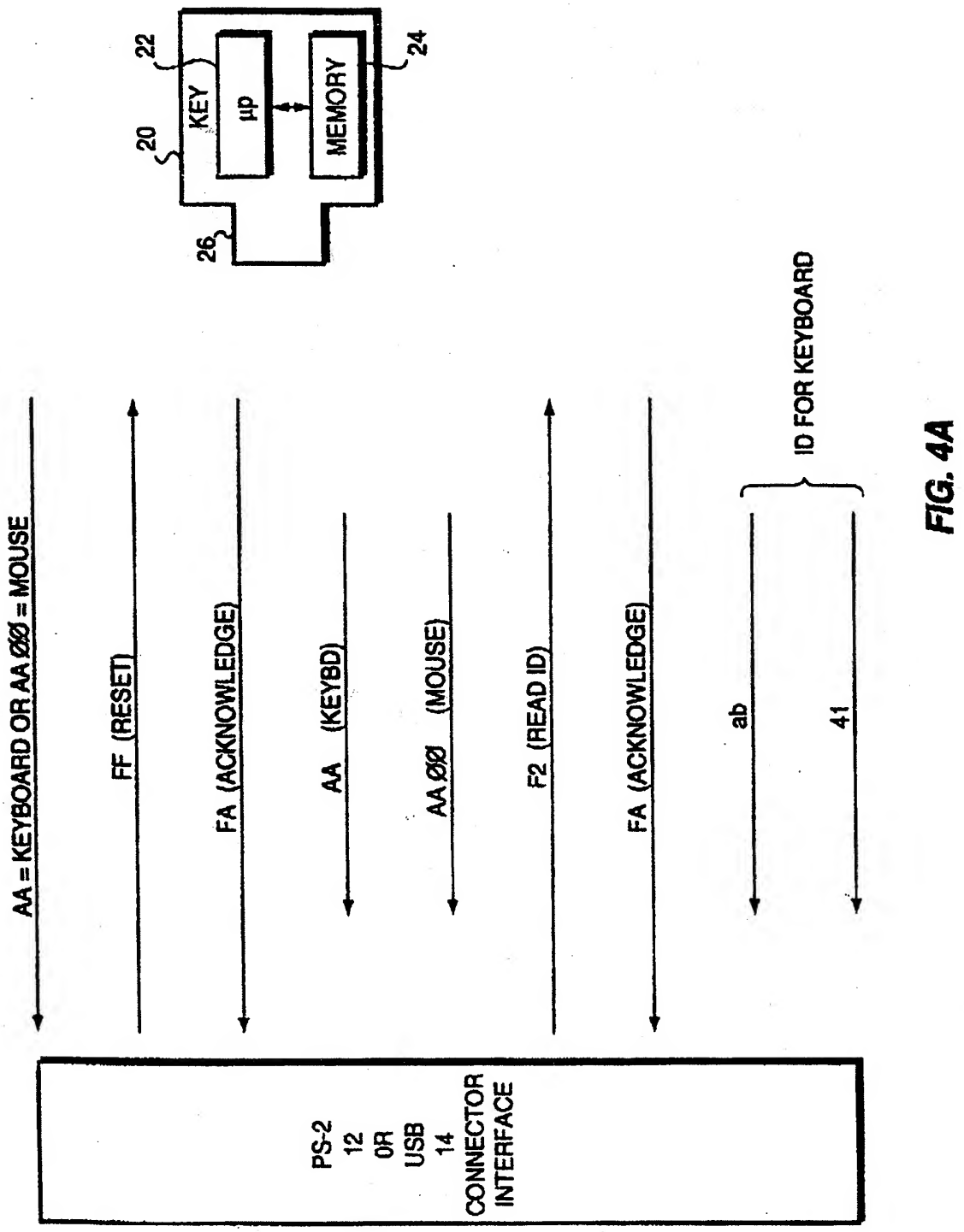


FIG. 4A

BNSDOCID: <WO_____0007088A1_I_>

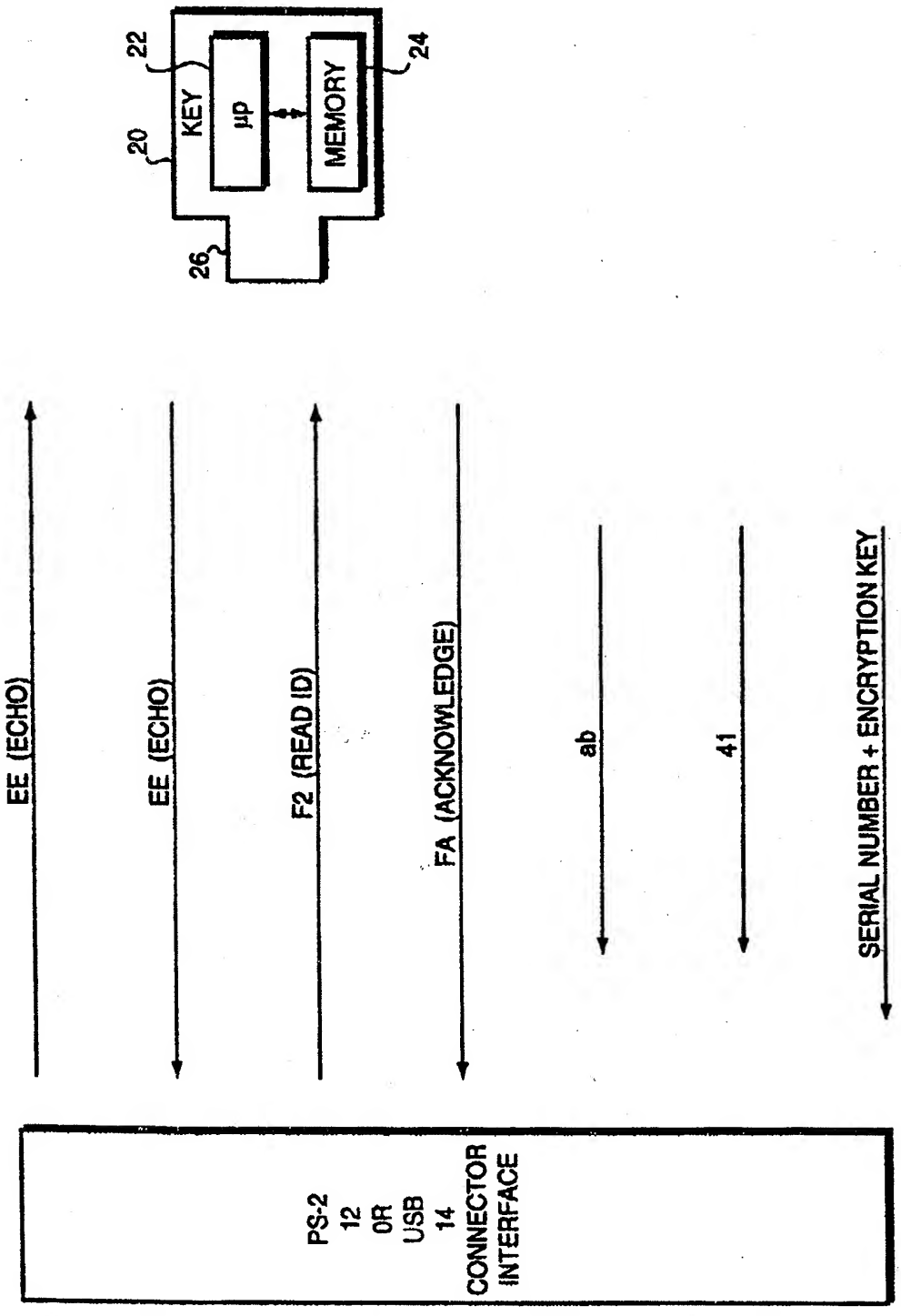
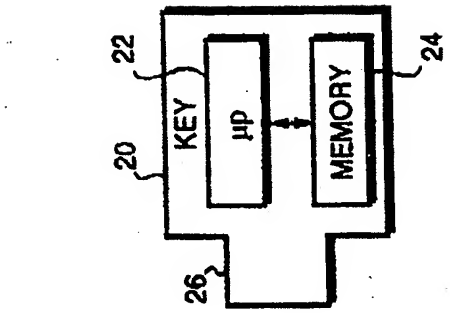


FIG. 4B

3NSDOCID: <WO_____0007088A1_I_>



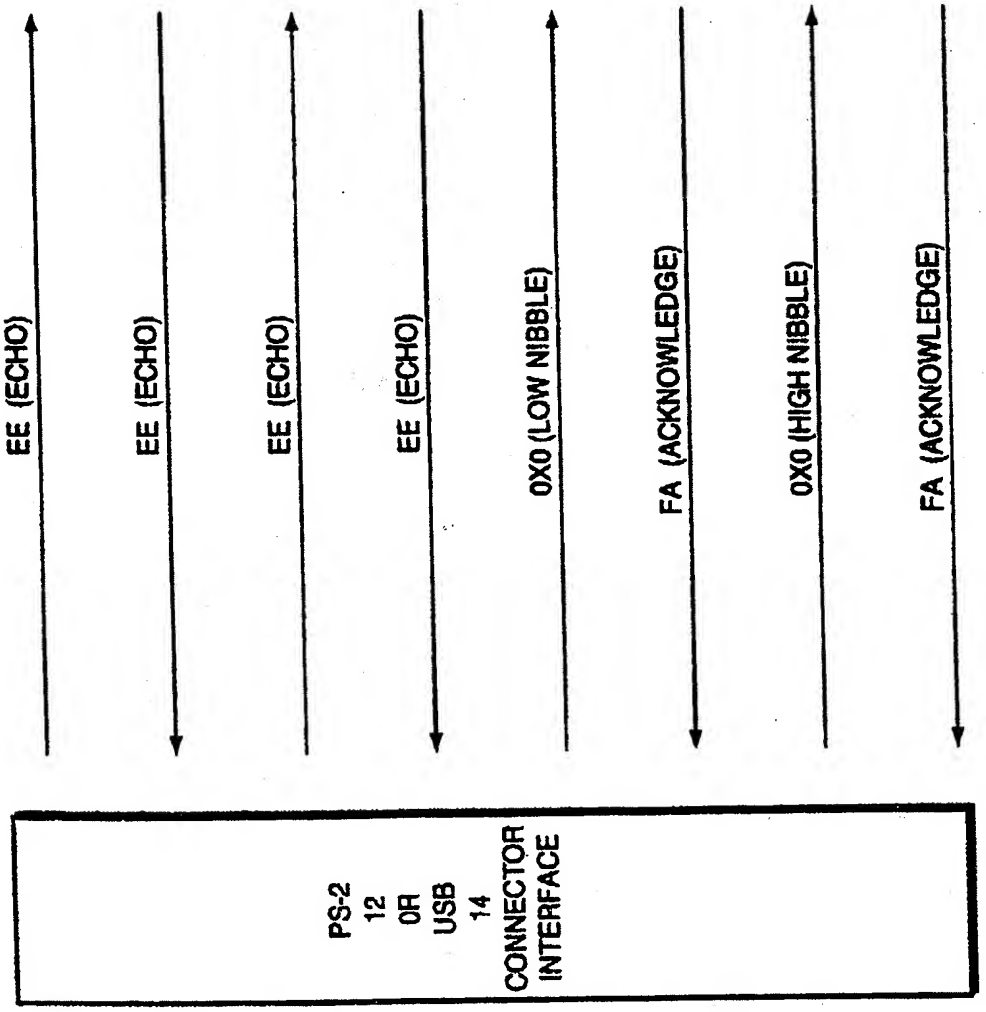


FIG. 4C

BNSDOCID: <WO_____0007088A1_I_>

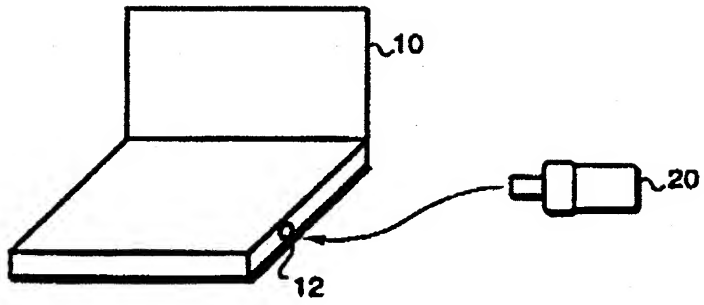


FIG. 5A

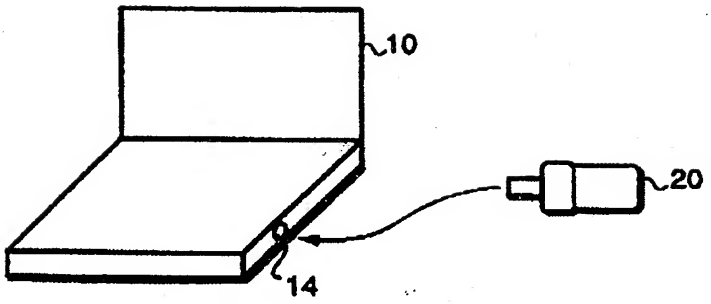


FIG. 5B

3NSDOCID: <WO_____0007088A1_I_>

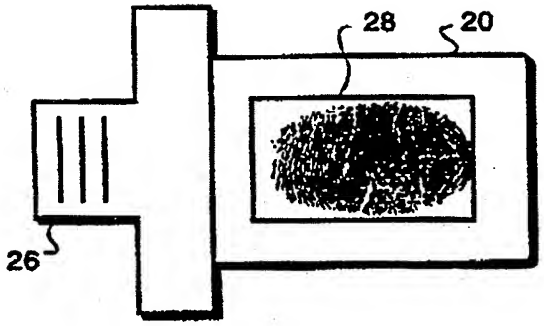


FIG. 5C

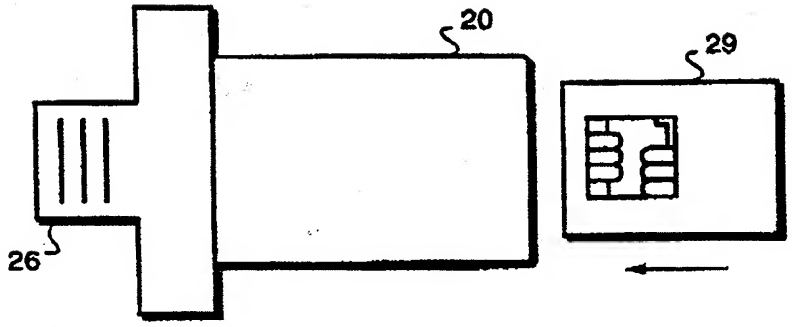


FIG. 5D

3NSDOCID: <WO_____0007088A1_I_>

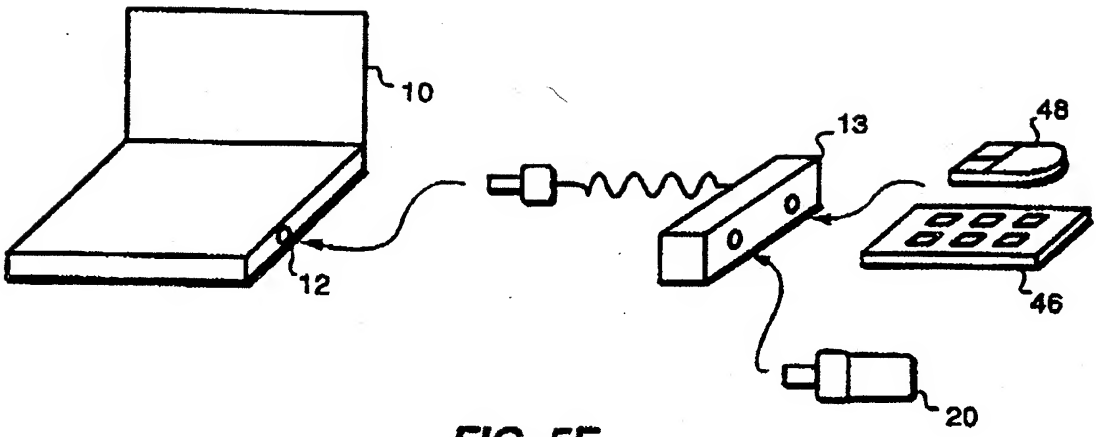


FIG. 5E

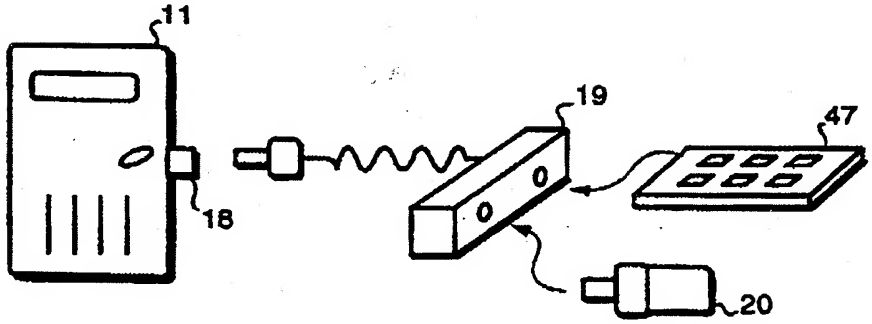


FIG. 5F

3NSDOCID: <WO_____0007088A1_I_>

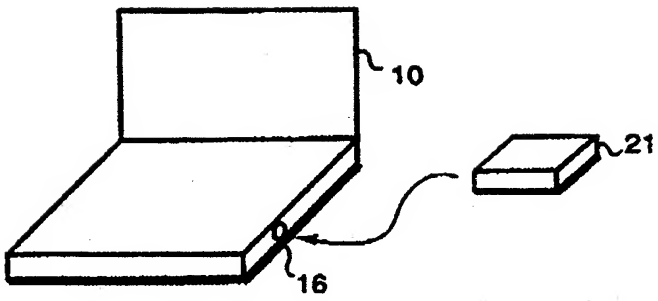


FIG. 6A

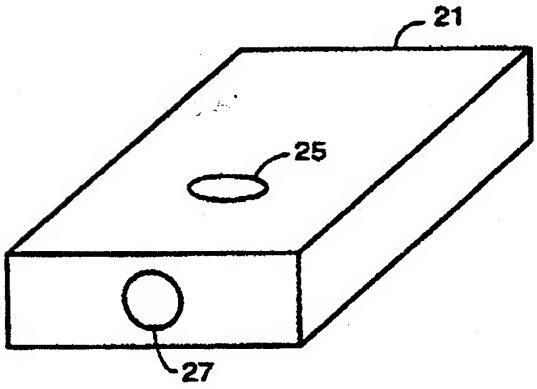


FIG. 6B

3NSDOCID: <WO_____0007088A1_I_>

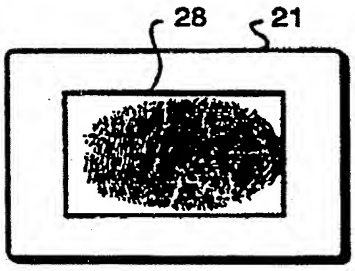


FIG. 6C

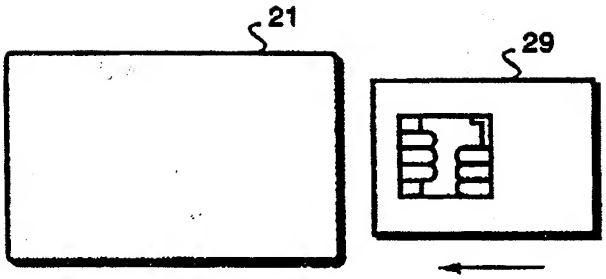


FIG. 6D

3NSDOCID: <WO_____0007088A1_I_>

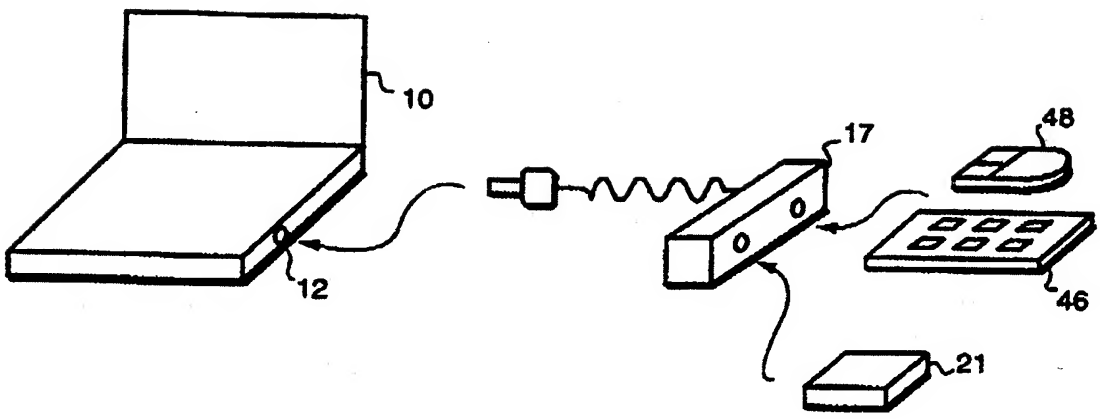


FIG. 6E

3NSDOCID: <WO_____0007088A1_I_>

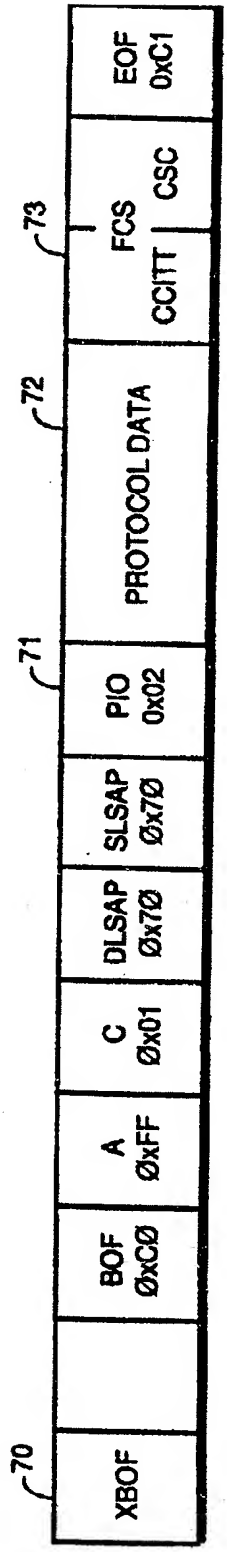


FIG. 7

3NSDOCID: <WO_____0007088A1_I_>

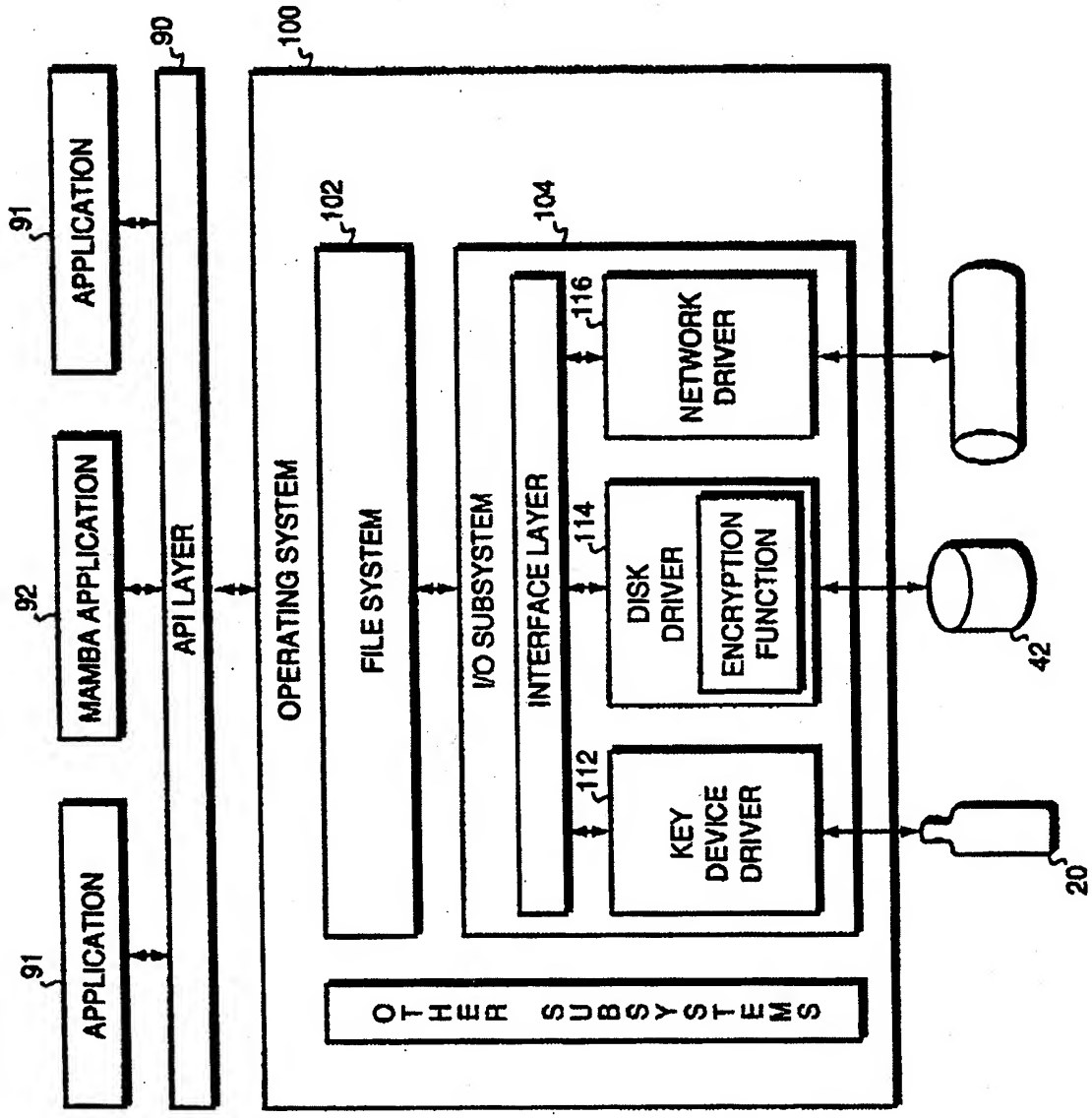


FIG. 8

BNSDOCID: <WO_____0007088A1_I_>

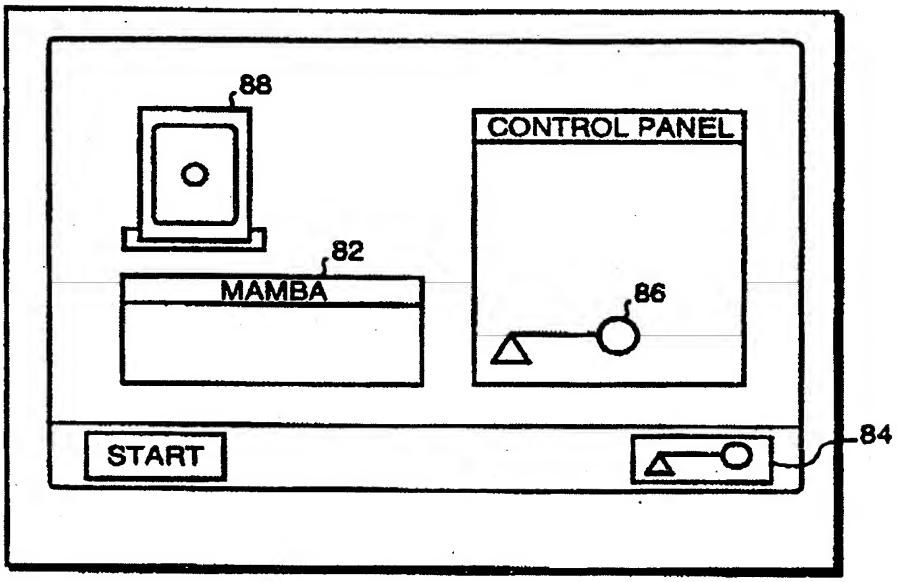


FIG. 9

3NSDOCID: <WO_____0007088A1_I_>

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/17315

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 606 615 A (LAPOINTE BRIAN K ET AL) 25 February 1997 (1997-02-25) figures 1-3 column 4, line 45 -column 8, line 54	1-6, 11-17
A	US 5 402 492 A (GOODMAN MICHAEL K ET AL) 28 March 1995 (1995-03-28) figures 1,2 column 4, line 6 -column 1120	1-3,5,6, 8,11-14, 16,17

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 1999	10/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

BNSDOCID: <WO_____0007088A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

Ir tional Application No
PCT/US 99/17315

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5606615 A	25-02-1997	NONE	
US 5402492 A	28-03-1995	NONE	

3NSDOCID: <WO_____0007088A1_I_>